Program Directory for

IBM Enhanced Access Control for SCLM for z/OS

Release 1, Modification Level 0

Program Number 5697-H59

FMID H278110

for Use with
OS/390 Version 2 Release 10 or later
z/OS Version 1 Release 1 or later

Document Date: September 2002

GI10-8450-00

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page v.

A form for reader's comments appears at the back of this publication. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Notices

References in this document to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

APAR numbers are provided in this document to assist in locating PTFs that may be required. Ongoing problem reporting may result in additional APARs being created. Therefore, the APAR lists in this document may not be complete. To obtain current service recommendations and to identify current product service requirements, always contact the IBM Customer Support Center or use S/390 SoftwareXcel to obtain the current "PSP Bucket".

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, New York 10504-1785
USA

For online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

CBPDO	SCLM	OS/390
IBM®	z/OS	S/390
RACF		

1.0 Introduction

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Enhanced Access Control for SCLM for z/OS. This publication refers to IBM Enhanced Access Control for SCLM for z/OS as Enhanced Access Control. You should read all of this program directory before installing the program and then keep it for future reference.

The program directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic and optional program materials and documentation for Enhanced Access Control.
- 3.0, “Program Support” on page 6 describes the IBM support available for Enhanced Access Control.
- 4.0, “Program and Service Level Information” on page 7 lists the APARs (program level) and PTFs (service level) incorporated into Enhanced Access Control.
- 5.0, “Installation Requirements and Considerations” on page 8 identifies the resources and considerations for installing and using Enhanced Access Control.
- 6.0, “Installation Instructions” on page 13 provides detailed installation instructions for Enhanced Access Control. It also describes the procedures for activating the functions of Enhanced Access Control, or refers to appropriate publications.

Before installing Enhanced Access Control, read 3.2, “Preventive Service Planning” on page 6. This section tells you how to find any updates to the information and procedures in this program directory.

Do not use this program directory if you are installing Enhanced Access Control with a SystemPac or ServerPac. When using these offerings, use the jobs and documentation supplied with the offering. This documentation may point you to specific sections of the program directory as required.

If you are installing Enhanced Access Control using the Custom-Built Product Delivery Offering (CBPDO, 5751-CS3), a softcopy program directory is provided on the CBPDO tape which is identical to the printed copy shipped with your order. Your CBPDO contains a softcopy preventive service planning (PSP) upgrade for this product. All service and HOLDDATA for Enhanced Access Control are included on the CBPDO tape.

1.1 Enhanced Access Control Description

Enhanced Access Control for Software Configuration Library Manager (SCLM) for z/OS is a new product in the SCLM Suite family. Enhanced Access Control for SCLM provides improved granularity and protection for SCLM datasets so that modifications can be made only by an authorized SCLM user. Authorization is required for any modification to the SCLM controlled libraries, whether made via native SCLM, or via tools which use standard SCLM services to access and update these SCLM datasets. Enhanced Access Control allows the addition of new rules that specify exactly which programs can be

used to access which datasets, thereby adding the flexibility to define specific users read or write access to specific documents. Validation profiles, accessing programs, and user or user group privileges can be defined through a menu driven end-user interface.

1.2 Enhanced Access Control FMIDs

Enhanced Access Control consists of the following FMIDs:

H278110

2.0 Program Materials

An IBM program is identified by a program number and a feature number. The program number for Enhanced Access Control is 5697-H59.

Basic Machine-Readable Materials are materials that are supplied under the base license and feature code, and are required for the use of the product. Optional Machine-Readable Materials are orderable under separate feature codes, and are not required for the product to function.

The program announcement material describes the features supported by Enhanced Access Control. Ask your IBM representative for this information if you have not already received a copy.

2.1 Basic Machine-Readable Material

The distribution medium for this program is magnetic tape or downloadable files. It is installed using SMP/E, and is in SMP/E RELFILE format. See 6.0, “Installation Instructions” on page 13 for more information about how to install the program.

Figure 1 describes the physical tape. Figure 2 describes the file content.

Notes:

1. The data set attributes in these tables should be used in the JCL of jobs reading the data sets, but since the data sets are in IEBCOPY unloaded format, their actual attributes may be different.
2. If you are installing Enhanced Access Control using the Custom-Built Product Delivery Offering (CBPDO) (5751-CS3), some of the information in these figures may not be valid. Consult the CBPDO documentation for actual values.
3. If any RELFILEs are identified as PDSEs, ensure that SMPTLIB data sets are allocated as PDSEs.

Figure 1. Basic Material: Program Tape

Medium	Feature Number	Physical Volume	External Label	R/M *	VOLSER
3480	5802	1	EAC for SCLM	N	278110

* R/M = Restricted Materials of IBM

Figure 2. Program File Content

Name	ORG	RECFM	LRECL	BLK SIZE
SMPMCS	SEQ	FB	80	6160
IBM.H278110.F1	PDS	FB	80	6160
IBM.H278110.F2	PDS	U	0	6144
IBM.H278110.F3	PDS	FB	80	6160
IBM.H278110.F4	PDS	FB	80	6160
IBM.H278110.F5	PDS	FB	80	6160
IBM.H278110.F6	PDS	FB	80	6160
IBM.H278110.F7	PDS	FB	80	6160
IBM.H278110.F8	PDS	VB	7896	7900
IBM.H278110.F9	PDS	FB	80	6160

2.2 Optional Machine-Readable Material

No optional machine-readable materials are provided for Enhanced Access Control.

2.3 Program Publications

The following sections identify the basic and optional publications for Enhanced Access Control.

2.3.1 Basic Program Publications

Figure 3 identifies the basic unlicensed program publications for Enhanced Access Control. One copy of each of these publications is included when you order the basic materials for Enhanced Access Control. For additional copies, contact your IBM representative.

Figure 3. Basic Material: Unlicensed Publications

Publication Title	Form Number
Enhanced Access Control for SCLM Users Guide	SC27-1591

2.3.2 Optional Program Publications

No optional publications are provided for Enhanced Access Control.

2.4 Program Source Materials

No program source materials or viewable program listings are provided for Enhanced Access Control.

2.5 Publications Useful During Installation

The publications listed in Figure 4 may be useful during the installation of Enhanced Access Control. To order copies, contact your IBM representative or visit the IBM Publications Center on the world wide web at: elink.ibmlink.ibm.com/applications/public/applications/publications/ cgibin/pbi.cgi on the Internet.

Figure 4. Publications Useful During Installation

Publication Title	Form Number
IBM SMP/E for z/OS and OS/390 User's Guide	SA22-7773
IBM SMP/E for z/OS and OS/390 Commands	SA22-7771
IBM SMP/E for z/OS and OS/390 Reference	SA22-7772
IBM SMP/E for z/OS and OS/390 Messages, Codes, and Diagnosis	GA22-7770
z/OS Secureway Security Server RACF Systems Programmers Guide	SA22-7681
z/OS Secureway Security Server RACF Security Administrators Guide	SA22-7683

3.0 Program Support

This section describes the IBM support available for Enhanced Access Control.

3.1 Program Services

Contact your IBM representative for specific information about available program services.

3.2 Preventive Service Planning

Before installing Enhanced Access Control, you should review the current Preventive Service Planning (PSP) information. If you obtained Enhanced Access Control as part of a CBPDO, there is HOLDDATA and PSP information included on the CBPDO.

If you obtained Enhanced Access Control on a product tape, or if the CBPDO is more than two weeks old when you install it, you should contact the IBM Support Center or use S/390 SoftwareXcel to obtain the current "PSP Bucket".

For access to RETAIN, visit http://www.ibmlink.ibm.com/ on the Internet.

PSP Buckets are identified by UPGRADEs, which specify product levels, and SUBSETs, which specify the FMIDs for a product level. The UPGRADE and SUBSET values for Enhanced Access Control are:

Figure 5. PSP Upgrade and Subset ID

UPGRADE	SUBSET	Description
EACSCLM	H278110	Enhanced Access Control for SCLM 1.1.0

3.3 Statement of Support Procedures

Report any difficulties you have using this program to your IBM Support Center. If an APAR is required, the Support Center will provide the address to which any needed documentation can be sent.

Figure 6 identifies the component IDs (COMPID) for Enhanced Access Control.

Figure 6. Component IDs

FMID	COMPID	Component Name	RETAIN Release
H278110	5697H5900	Enhanced Access Control for SCLM	110

4.0 Program and Service Level Information

This section identifies the program and any relevant service levels of Enhanced Access Control. The program level refers to the APAR fixes incorporated into the program. The service level refers to the PTFs integrated.

4.1 Program Level Information

No APARs have been incorporated into Enhanced Access Control.

4.2 Service Level Information

No PTFs against this release of Enhanced Access Control have been incorporated into the product tape.

5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating Enhanced Access Control. The following terminology is used:

- *Driving system*: the system used to install the program.
- *Target system*: the system on which the program is installed.

In many cases, the same system can be used as both a driving system and a target system. However, you may want to set up a clone of your system to use as a target system by making a separate IPL-able copy of the running system. The clone should include copies of all system libraries that SMP/E updates, copies of the SMP/E CSI data sets that describe the system libraries, and your PARMLIB and PROCLIB.

Some cases where two systems should be used include the following:

- When installing a new level of a product that is already installed, the new product will delete the old one. By installing onto a separate target system, you can test the new product while still keeping the old one in production.
- When installing a product that shares libraries or load modules with other products, the installation can disrupt the other products. Installing onto a test system or clone will allow you to assess these impacts without disrupting your production system.

5.1 Driving System Requirements

This section describes the environment of the driving system required to install Enhanced Access Control.

5.1.1 Machine Requirements

The driving system can run in any hardware environment that supports the required software.

5.1.2 Programming Requirements

Figure 7. Driving System Software Requirements

Program Number	Product Name and Minimum VRM/Service Level
Any **one** of the following:	
5647-A01	OS/390 SMP/E Version 2 Release 10 or higher
5694-A01	z/OS Version 1 Release 1 or higher
5655-G44	IBM SMP/E for z/OS and OS/390 Version 3 Release 1 or higher

5.2 Target System Requirements

This section describes the environment of the target system required to install and use Enhanced Access Control.

Enhanced Access Control installs in the MVS (Z038) SREL.

5.2.1 Machine Requirements

The target system can run in any hardware environment that supports the required software.

5.2.2 Programming Requirements

5.2.2.1 Mandatory Requisites: A mandatory requisite is defined as a product that is required without exception; this product either **will not install** or **will not function** unless this requisite is met. This includes products that are specified as REQs or PREs.

Enhanced Access Control has no mandatory requisites.

5.2.2.2 Functional Requisites: A functional requisite is defined as a product that is **not** required for the successful installation of this product or for the basic function of the product, but **is** needed at run time for a specific function of this product to work. This includes products that are specified as IF REQs.

Enhanced Access Control has no functional requisites.

5.2.2.3 Toleration/Coexistence Requisites: A toleration/coexistence requisite is defined as a product which must be present on a sharing system. These systems can be other systems in a multisystem environment (not necessarily sysplex), a shared DASD environment (such as test and production), or systems that reuse the same DASD at different time intervals.

Enhanced Access Control has no toleration/coexistence requisites.

5.2.2.4 Incompatibility (Negative) Requisites: A negative requisite identifies products which must *not* be installed on the same system as this product.

Enhanced Access Control has no negative requisites.

5.2.3 DASD Storage Requirements

Enhanced Access Control libraries can reside on all supported DASD types.

Figure 8 lists the total space required for each type of library.

Figure 8. Total DASD Space Required by Enhanced Access Control

Library Type	Total Space Required
Target	100 tracks (3390)
Distribution	100 tracks (3390)

Notes:

1. IBM recommends use of system determined block sizes for efficient DASD utilization for all non-RECFM U data sets. For RECFM U data sets, IBM recommends a block size of 32760, which is the most efficient from a performance and DASD utilization perspective.
2. Abbreviations used for the data set type are:

   U Unique data set, allocated by this product and used only by this product. To determine the correct storage needed for this data set, this table provides all required information; no other tables (or program directories) need to be referenced for the data set size.

   S Shared data set, allocated by this product and used by this product and others. To determine the correct storage needed for this data set, the storage size given in this table needs to be added to other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

   E Existing shared data set, used by this product and others. This data set is NOT allocated by this product. To determine the correct storage needed for this data set, the storage size given in this table needs to be added to other tables (perhaps in other program directories). This existing data set must have enough free space to accommodate the storage size given in this table.

   If you currently have a previous release of this product installed in these libraries, the installation of this release will delete the old one and reclaim the space used by the old release and any service that had been installed. You can determine whether or not these libraries have enough space by deleting the old release with a dummy function, compressing the libraries, and comparing the space requirements with the free space in the libraries.

   For more information on the names and sizes of the required data sets, please refer to 6.1.5, “Allocate SMP/E Target and Distribution Libraries and Paths” on page 15.
3. All target and distribution libraries listed have the following attributes:
   - The default name of the data set may be changed
   - The default block size of the data set may be changed
   - The data set may be merged with another data set that has equivalent characteristics
   - The data set may be either a PDS or a PDSE
4. All target libraries listed have the following attributes:
   - The data set may be SMS managed
   - It is not required for the data set to be SMS managed
   - It is not required for the data set to reside on the IPL volume

- The values in the "Member Type" column are not necessarily the actual SMP/E element types identified in the SMPMCS.

The following figures describe the target and distribution libraries required to install Enhanced Access Control. The storage requirements of Enhanced Access Control must be added to the storage required by other programs having data in the same library or path.

Note: The data in these tables should be used when determining which libraries can be merged into common data sets. In addition, since some ALIAS names may not be unique, ensure that no naming conflicts will be introduced before merging libraries.

Figure 9. Storage Requirements for Enhanced Access Control Target Libraries

Library DDNAME	Member Type	Target Volume	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
SHSSJCL	Sample	ANY	U	PDS	FB	80	2	5
SHSSLINK	LMOD	ANY	U	PDS	U	0	25	10
SHSSPENU	Panel	ANY	U	PDS	FB	80	40	10
SHSSMENU	Message	ANY	U	PDS	FB	80	2	5
SHSSTENU	Table	ANY	U	PDS	FB	80	2	5
SHSSEXEC	EXEC	ANY	U	PDS	FB	80	6	5
SHSSSAMP	Sample	ANY	U	PDS	FB	80	2	5
SHSSDATA	Data	ANY	U	PDS	VB	7896	5	5

Figure 10. Storage Requirements for Enhanced Access Control Distribution Libraries

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
AHSSJCL	U	PDS	FB	80	2	5
AHSSLOAD	U	PDS	U	0	25	10
AHSSPENU	U	PDS	FB	80	40	10
AHSSMENU	U	PDS	FB	80	2	5
AHSSTENU	U	PDS	FB	80	2	5
AHSSEXEC	U	PDS	FB	80	6	5
AHSSSAMP	U	PDS	FB	80	2	5
AHSSDATA	U	PDS	VB	7896	5	5

5.3 FMIDs Deleted

Installing Enhanced Access Control may result in the deletion of other FMIDs. To see what FMIDs will be deleted, examine the ++VER statement in the product's SMPMCS.

If you do not wish to delete these FMIDs at this time, you must install Enhanced Access Control into separate SMP/E target and distribution zones.

Note: These FMIDs will not automatically be deleted from the Global Zone. Consult the SMP/E manuals for instructions on how to do this.

5.4 Special Considerations

Enhanced Access Control has no special considerations for the target system.

6.0 Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of Enhanced Access Control.

Please note the following:

- If you want to install Enhanced Access Control into its own SMP/E environment, consult the SMP/E manuals for instructions on creating and initializing the SMPCSI and the SMP/E control data sets. If required a sample job HSSALSMP has been supplied to assist in creating its own SMP/E environment.
- Sample jobs have been provided to help perform some or all of the installation tasks. The SMP/E jobs assume that all DDDEF entries required for SMP/E execution have been defined in the appropriate zones.
- The SMP/E dialogs may be used instead of the sample jobs to accomplish the SMP/E installation steps.

6.1 Installing Enhanced Access Control

6.1.1 SMP/E Considerations for Installing Enhanced Access Control

This release of Enhanced Access Control is installed using the SMP/E RECEIVE, APPLY, and ACCEPT commands. The SMP/E dialogs may be used to accomplish the SMP/E installation steps.

6.1.2 SMP/E Options Subentry Values

The recommended values for some SMP/E CSI subentries are shown in Figure 11. Use of values lower than these may result in failures in the installation process. DSSPACE is a subentry in the GLOBAL options entry. PEMAX is a subentry of the GENERAL entry in the GLOBAL options entry. Refer to the SMP/E manuals for instructions on updating the global zone.

Figure 11. SMP/E Options Subentry Values

SUB-ENTRY	Value	Comment
DSSPACE	300,50,250	Space allocation for TLIB data sets.
PEMAX	SMP/E Default	IBM recommends using the SMP/E default for PEMAX.

6.1.3 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install Enhanced Access Control:

Figure 12. Sample Installation Jobs

Job Name	Job Type	Description	RELFILE
HSSALSMP	SMP/E	(Optional) Sample job to define and initialize an SMP/E environment.	IBM.H278110.F1
HSSRECEV	RECEIVE	Sample RECEIVE job	IBM.H278110.F1
HSSALLOC	ALLOCATE	Sample job to allocate target and distribution libraries	IBM.H278110.F1
HSSDDDEF	DDDEF	Sample job to define SMP/E DDDEFs	IBM.H278110.F1
HSSAPPLY	APPLY	Sample APPLY job	IBM.H278110.F1
HSSACCEP	ACCEPT	Sample ACCEPT job	IBM.H278110.F1

You may copy the jobs from the tape or product files by submitting the job below. Use either the //TAPEIN or the //FILEIN DD statement, depending on your distribution medium, and comment out or delete the other statement. Add a job card and change the lowercase parameters to uppercase values to meet your site's requirements before submitting.

```
//STEP1    EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//TAPEIN   DD DSN=IBM.H278110.F1,UNIT=tunit,VOL=SER=278110,
//         LABEL=(2,SL),DISP=(OLD,KEEP)
//FILEIN   DD DSN=IBM.H278110.F1,UNIT=SYSALLDA,DISP=SHR,
//         VOL=SER=filevol
//OUT      DD DSNAME=jcl-library-name,
//         DISP=(NEW,CATLG,DELETE),
//         VOL=SER=dasdvol,UNIT=SYSALLDA,
//         SPACE=(TRK,(2,1,1))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD *
    COPY INDD=xxxxIN,OUTDD=OUT
/*
```

where **tunit** is the unit value matching the product tape, **filevol** is the volume serial of the DASD device where the downloaded files reside, **jcl-library-name** is the name of the output data set where the sample jobs will be stored, **dasdvol** is the volume serial of the DASD device where the output data set will reside and **xxxxIN** on the SYSIN DD to either TAPEIN or FILEIN depending on your input DD statement.

You can also access the sample installation jobs by performing an SMP/E RECEIVE and then copying the jobs from the SMPTLIBs to a work data set for editing and submission. See Figure 12 on page 13 to find the appropriate SMPTLIB data set.

6.1.4 Perform SMP/E RECEIVE

Edit and submit sample job HSSRECEV to perform the SMP/E RECEIVE for Enhanced Access Control. Consult the instructions in the sample job for more information.

NOTE: If you obtained Enhanced Access Control as part of a CBPDO, you can use the RCVPDO job found in the CBPDO RIMLIB data set to RECEIVE the Enhanced Access Control FMIDs as well as any service, HOLDDATA, or preventive service planning (PSP) information included on the CBPDO tape. For more information, refer to the documentation included with the CBPDO.

Expected Return Codes and Messages: This job should issue a return code of zero and no error messages.

6.1.5 Allocate SMP/E Target and Distribution Libraries and Paths

Edit and submit sample job HSSALLOC to allocate the SMP/E target and distribution libraries for Enhanced Access Control. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: This job should issue a return code of zero and no error messages.

6.1.6 Create DDDEF Entries

Edit and submit sample job HSSDDDEF to create DDDEF entries for the SMP/E target and distribution libraries for Enhanced Access Control. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: This job should issue a return code of zero and no error messages.

6.1.7 Perform SMP/E APPLY

Edit and submit sample job HSSAPPLY to perform an SMP/E APPLY CHECK for Enhanced Access Control. Consult the instructions in the sample job for more information.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the following on the APPLY CHECK: PRE, ID, REQ, and IFREQ. This is because the SMP/E root cause analysis identifies the cause only of **ERRORS** and not of **WARNINGS** (SYSMODs that are bypassed are treated as warnings, not errors, by SMP/E).

Once you have taken any actions indicated by the APPLY CHECK, remove the CHECK operand and run the job again to perform the APPLY.

Note: The GROUPEXTEND operand indicates that SMP/E apply all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

Expected Return Codes and Messages from APPLY CHECK: This job should issue a return code of zero and no error messages.

Expected Return Codes and Messages from APPLY: This job should issue a return code of zero and no error messages.

6.1.8 Perform SMP/E ACCEPT

Edit and submit sample job HSSACCEP to perform an SMP/E ACCEPT CHECK for Enhanced Access Control. Consult the instructions in the sample job for more information.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the following on the ACCEPT CHECK: PRE, ID, REQ, and IFREQ. This is because the SMP/E root cause analysis identifies the cause only of **ERRORS** and not of **WARNINGS** (SYSMODs that are bypassed are treated as warnings, not errors, by SMP/E).

Before using SMP/E to load new distribution libraries, it is recommended that you set the ACCJCLIN indicator in the distribution zone. This will cause entries produced from JCLIN to be saved in the distribution zone whenever a SYSMOD containing inline JCLIN is ACCEPTed. For more information on the ACCJCLIN indicator, see the description of inline JCLIN in the SMP/E manuals.

Once you have taken any actions indicated by the ACCEPT CHECK, remove the CHECK operand and run the job again to perform the ACCEPT.

Note: The GROUPEXTEND operand indicates that SMP/E accept all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

Expected Return Codes and Messages from ACCEPT CHECK: This job should issue a return code of zero and no error messages.

Expected Return Codes and Messages from ACCEPT: This job should issue a return code of zero and no error messages.

If PTFs containing replacement modules are being ACCEPTed, SMP/E ACCEPT processing will linkedit/bind the modules into the distribution libraries. During this processing, the Linkage Editor or Binder may issue messages documenting unresolved external references, resulting in a return code of 4 from the ACCEPT step. These messages can be ignored, because the distribution libraries are not executable and the unresolved external references will not affect the executable system libraries.

6.2 Activating Enhanced Access Control and further customization.

Enhanced Access Control is fully operational once the SMP/E installation and the POST-SMP/E customization referenced in the Users Guide is complete. Reference the Installation chapter in the Enhanced Access Control for SCLM for z/OS Users Guide to complete the customization. The Users Guide may be downloaded from the following website :
http://www.ibm.com/software/ad/sclmsuite/accesscontrol/

Reader's Comments

Program Directory for IBM Enhanced Access Control for SCLM for z/OS September 2002

You may use this form to comment about this document, its organization, or subject matter with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

For each of the topics below please indicate your satisfaction level by circling your choice from the rating scale. If a statement does not apply, please circle N.

RATING SCALE

```
  very                                  very          not
satisfied  <====================>  dissatisfied  applicable
    1        2        3        4         5            N
```

	Satisfaction					
Ease of product installation	1	2	3	4	5	N
Contents of program directory	1	2	3	4	5	N
Installation Verification Programs	1	2	3	4	5	N
Time to install the product	1	2	3	4	5	N
Readability and organization of program directory tasks	1	2	3	4	5	N
Necessity of all installation tasks	1	2	3	4	5	N
Accuracy of the definition of the installation tasks	1	2	3	4	5	N
Technical level of the installation tasks	1	2	3	4	5	N
Ease of getting the system into production after installation	1	2	3	4	5	N

How did you order this product?

___ CBPDO
___ CustomPac
___ ServerPac
___ Independent
___ Other

Is this the first time your organization has installed this product?

___ Yes
___ No

Were the people who did the installation experienced with the installation of z/OS products?

___ Yes

__ No

If yes, how many years? __

If you have any comments to make about your ratings above, or any other aspect of the product installation, please list them below:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Please provide the following contact information:

_____
Name and Job Title

_____
Organization

_____

_____
Address

_____
Telephone

Thank you for your participation.

Please send the completed form to (or give to your IBM representative who will forward it to the IBM Enhanced Access Control for SCLM for z/OS Development group):

Australian Programming Centre
IBM Global Services Australia
1060 Hay Street
West Perth
WA 6005
AUSTRALIA

FAX Number: +61-8-9261-8453

Printed in U.S.A.

GI10-8450-00